Système d'information sur les services à domicile

Évaluation des incidences sur la vie privée du, juin 2022

Juin 2022

Institut canadien d'information sur la santé
Canadian Institute for Health Information

La production du présent document est rendue possible grâce à un apport financier de Santé Canada et des gouvernements provinciaux et territoriaux. Les opinions exprimées dans ce rapport ne représentent pas nécessairement celles de Santé Canada ou celles des gouvernements provinciaux et territoriaux.

Institut canadien d'information sur la santé
495, chemin Richmond, bureau 600
Ottawa (Ontario) K2A 4H6
Téléphone : 613-241-7860
Télécopieur : 613-241-8120
icis.ca
droitauteur@icis.ca

Comment citer ce document :
Institut canadien d'information sur la santé. *Système d'information sur les services à domicile : évaluation des incidences sur la vie privée du, juin 2022*.
Ottawa, ON : ICIS; 2022.

This publication is also available in English under the title *Home Care Reporting System Privacy Impact Assessment, June 2022*.

L'Institut canadien d'information sur la santé (ICIS) est fier de publier l'évaluation des incidences sur la vie privée suivante conformément à sa *Politique d'évaluation des incidences sur la vie privée* :

- *Système d'information sur les services à domicile : évaluation des incidences sur la vie privée du, juin 2022*

Approuvée par

Brent Diverty
Vice-président, Stratégies de données et Statistiques

Rhonda Wing
Directrice exécutive, chef de la protection des renseignements personnels et avocate générale

Ottawa, juin 2022

Table des matières

Le Système d'information sur les services à domicile en bref

1. Le Système d'information sur les services à domicile (SISD) est une base de données pancanadienne qui contient des renseignements normalisés sur les services à domicile financés par le secteur public.
2. Les organismes recueillent des données dans le cadre de la prestation des soins avant de les soumettre au SISD.
3. L'ICIS utilise les données du SISD pour dégager de l'information exacte, actuelle et comparable sur les populations de clients qui reçoivent des services à domicile, sur les services dispensés et sur les résultats pour les clients.

1 Introduction

L'Institut canadien d'information sur la santé (ICIS) recueille et analyse de l'information sur la santé et les soins de santé au Canada. Son mandat consiste à fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l'ensemble du continuum de soins. L'ICIS obtient des données des hôpitaux et d'autres établissements de santé, des établissements de soins de longue durée, des autorités sanitaires régionales, des praticiens et des gouvernements. Ces données comprennent des renseignements sur les services de santé dispensés aux patients, sur les professionnels de la santé qui dispensent ces services et sur le coût des services de santé.

La présente évaluation des incidences sur la vie privée a pour but d'examiner les risques liés au respect de la vie privée, à la confidentialité et à la sécurité associés au Système d'information sur les services à domicile (SISD). Elle remplace la version de 2016 et consiste en un examen des 10 principes énoncés dans le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation et de la façon dont ils s'appliquent au SISD. Elle analyse aussi l'application du *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* de l'ICIS.

Cette évaluation vise avant tout à respecter la *Politique d'évaluation des incidences sur la vie privée* de l'ICIS.

2 Contexte

Le SISD est une base de données pancanadienne qui contient des renseignements normalisés sur les services à domicile financés par le secteur public. Il sert à recueillir les données sur les services à domicile fournis par les organismes publics ainsi que par les organismes privés mandatés par le gouvernement. Il contient des données sur les services à domicile de courte durée (p. ex. pour les clients souffrant d’une affection aiguë de durée limitée) et de longue durée (p. ex. pour les clients qui nécessitent un soutien prolongé pour pouvoir demeurer dans la collectivité). Le SISD contient également des données sur les évaluations visant les services à domicile financés par le secteur public, même pour les personnes n’ayant pas reçu, en fin de compte, de services à domicile. Toutefois, il ne permet pas de saisir des données sur les services à domicile financés par des fonds privés ou dispensés dans un cadre informel (p. ex. par des membres de la famille).

L’ICIS utilise les données du SISD pour dégager de l’information exacte, actuelle et comparable sur les populations de clients qui reçoivent des services à domicile, sur les services dispensés et sur les résultats pour les clients.

Le SISD ne sera pas opérationnel indéfiniment. Alors que les provinces et territoires commencent à utiliser les outils de collecte de données les plus récents, le SISD sera abandonné au profit du Système d’information intégré interRAI (SIIR), qui est conçu pour prendre en charge les nouveaux outils. Dès que l’ensemble des provinces et territoires seront passés au SIIR, le SISD sera mis hors service.

2.1 Collecte de données

En étroite collaboration avec les intervenants[i], l’ICIS choisit les éléments de données recueillis dans le SISD en fonction des meilleures données probantes disponibles concernant leur utilité et leur spécificité. Plus précisément, l’ICIS et les intervenants ont choisi l’instrument d’évaluation des résidents — services à domicile (RAI-HC) et l’évaluation à l’accueil interRAI (EA interRAI) comme fondement des normes de collecte de données du SISD. Ces 2 instruments d’évaluation ont été élaborés par interRAI, un réseau regroupant des chercheurs et des praticiens dont l’objectif est d’améliorer les soins de santé pour les personnes handicapées ou présentant des besoins médicaux complexes. Ces instruments d’évaluation sont le fruit de recherches et de tests rigoureux menés, entre autres, dans le but d’établir la fiabilité et la validité des éléments de données, des mesures des résultats

i. Par exemple, les ministères de la Santé qui demandent aux organismes de services à domicile qu’ils financent de soumettre des données au SISD, et le Comité consultatif sur les services à domicile et les soins de longue durée, qui représente les ministères de la Santé de façon générale.

pour les clients et de la catégorisation des clients selon l'utilisation des ressources et des indicateurs de la qualité des soins. À l'aide des instruments d'évaluation interRAI, les organismes recueillent des données dans le cadre de la prestation des soins avant de les soumettre au SISD. Chaque enregistrement soumis au SISD respecte les exigences du fichier minimal du SISD et comprend des identificateurs du client, des renseignements démographiques à son sujet, ses caractéristiques de santé, des données administratives et des champs de texte libre. De plus amples renseignements sur les éléments de données du fichier minimal du SISD sont accessibles sur le site Web de l'ICIS.

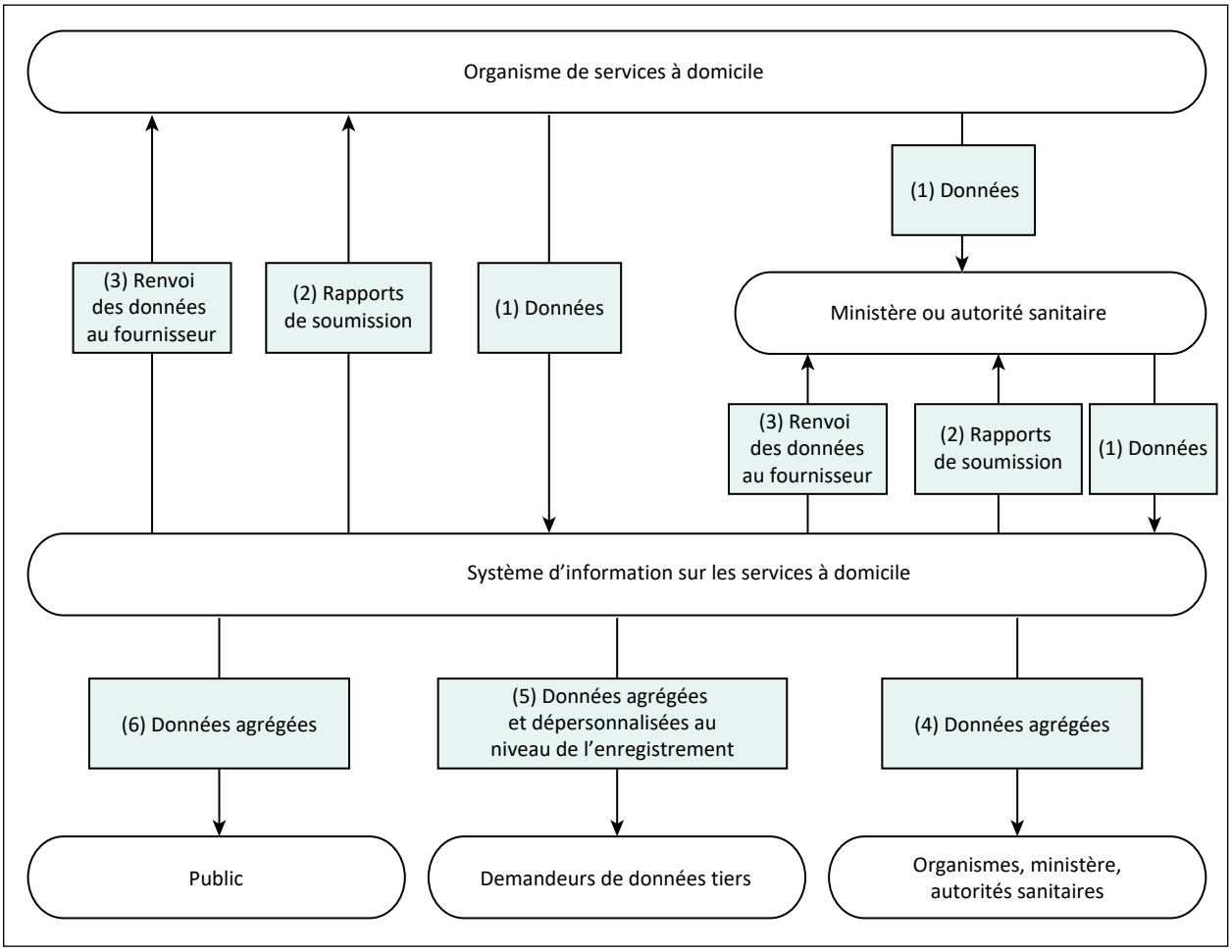
2.2 Cheminement des données

Le cheminement des données du SISD va comme suit :

1. L'organisme soumet les enregistrements à l'ICIS. Dans certains cas, les enregistrements sont soumis par un ministère ou une autorité sanitaire.
2. Le SISD transmet des rapports de soumission pour aider l'organisme à corriger les erreurs relevées dans les enregistrements (p. ex. éléments de données manquants).
3. Une copie des enregistrements tels qu'ils ont été acceptés par le SISD ainsi que certains rapports qui comprennent des renseignements personnels sur la santé sont mis à la disposition de l'organisme, du ministère et de l'autorité sanitaire régionale, selon le cas.
4. L'ICIS fournit, au moyen des rapports électroniques du SISD, des données agrégées aux organismes qui soumettent des données au SISD, aux autorités sanitaires et au ministère.
5. Le SISD peut divulguer des données agrégées et dépersonnalisées au niveau de l'enregistrement aux tiers qui en font la demande.
6. Le SISD divulgue des données agrégées au public.

La figure ci-dessous illustre le cheminement des données du SISD.

Figure Cheminement des données du SISD



2.3 Gestion de l'accès et soumission des données

L'accès aux applications sécurisées de l'ICIS est régi par la Division de la gestion de produits et de l'expérience client de l'ICIS. Cette division gère l'autorisation et la révocation de l'accès aux applications sécurisées de l'ICIS conformément aux processus établis du système de gestion de l'accès (SGA).

Un logiciel extrait les données directement des enregistrements de l'organisme. Une fois authentifié dans le SGA de l'ICIS, l'organisme peut soumettre des données au niveau de l'enregistrement au SISD à l'aide du Service de soumission électronique de données (eDSS) sécurisé de l'ICIS.

3 Analyse du respect de la vie privée

3.1 Programme de gestion des risques liés au respect de la vie privée et à la sécurité

La gestion des risques liés au respect de la vie privée et à la sécurité est un processus officiel et reproductible qui vise la détection, l'évaluation, le traitement et la surveillance des risques dans le but de réduire au minimum la probabilité qu'ils se matérialisent ou leur éventuelle incidence. En 2015, l'ICIS a approuvé son *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité* et mis en œuvre la *Politique sur la gestion des risques liés au respect de la vie privée et à la sécurité* connexe. La chef de la protection des renseignements personnels et le chef de la sécurité de l'information de l'ICIS, en collaboration avec des membres de la direction, ont la responsabilité de détecter, d'évaluer, de traiter, de surveiller et d'examiner les risques en matière de respect de la vie privée et de sécurité.

Les risques liés au respect de la vie privée et à la sécurité peuvent être détectés de diverses façons, par exemple par des évaluations des incidences sur la vie privée. Une fois détectés, les risques sont inscrits au registre des risques liés au respect de la vie privée et à la sécurité, et reçoivent la cote **élevé**, **moyen** ou **faible** selon leur probabilité et leur incidence :

- **élevé :** la probabilité que le risque se manifeste est élevée, ou les mesures de contrôle et les stratégies ne sont pas fiables ou efficaces;
- **moyen :** la probabilité que le risque se manifeste est moyenne, ou les mesures de contrôle et les stratégies sont moyennement fiables ou efficaces;
- **faible :** la probabilité que le risque se manifeste est faible, ou les mesures de contrôle et les stratégies sont fiables et efficaces.

Le niveau de risque est calculé en fonction de la probabilité et de l'incidence du risque détecté. La cote de niveau du risque (faible, moyen ou élevé) définit le degré de risque. Un niveau de risque élevé est signe d'une menace grave qu'il est impératif de prendre immédiatement en charge. Une fois un premier traitement du risque effectué, le risque résiduel (nouveau calcul de la probabilité et de l'incidence du risque par suite du traitement) est évalué et comparé à l'énoncé sur la tolérance des risques liés au respect de la vie privée et à la sécurité de l'ICIS, qui stipule que l'ICIS a une faible tolérance à de tels risques. Si le niveau de risque résiduel demeure plus élevé que faible, un traitement supplémentaire est nécessaire jusqu'à l'obtention d'un risque faible, ou jusqu'à ce que le risque non traité ou résiduel soit accepté par le Comité exécutif de l'ICIS au nom de l'organisme.

Comme l'indique la section 3.4, l'ICIS entreprend actuellement un processus de gestion des risques liés au respect de la vie privée et à la sécurité portant sur les champs de texte libre.

Aucun autre risque lié au respect de la vie privée et à la sécurité n'a été détecté à la suite de la présente évaluation des incidences sur la vie privée.

3.2 Textes législatifs régissant les données du SISD

Généralités

L'ICIS se conforme à sa *Politique de respect de la vie privée, 2010* ainsi qu'à toute loi ou entente juridique sur la vie privée applicable.

Lois sur la protection de la vie privée

L'ICIS est un collecteur secondaire de données sur la santé, expressément à des fins de planification et de gestion du système de santé, ce qui comprend l'analyse statistique et la production de rapports. Il incombe aux fournisseurs de données de respecter les obligations légales de leur autorité compétente, selon le cas, au moment de la collecte des données.

Les provinces et territoires suivants disposent de lois sur la protection des renseignements personnels sur la santé : Terre-Neuve-et-Labrador, Île-du-Prince-Édouard, Nouvelle-Écosse, Nouveau-Brunswick, Ontario, Manitoba, Saskatchewan, Alberta, Yukon et Territoires du Nord-Ouest. Celles-ci octroient aux établissements l'autorisation de divulguer des renseignements personnels sur la santé sans le consentement des patients pour les besoins des systèmes de santé, sous réserve de certaines exigences. Par exemple, l'ICIS est reconnu comme une entité prescrite en vertu de la *Loi sur la protection des renseignements personnels sur la santé* de l'Ontario; les dépositaires de renseignements sur la santé de l'Ontario peuvent donc divulguer de tels renseignements à l'ICIS sans le consentement des patients en vertu de l'article 29, comme le prévoit l'alinéa 45(1) de la Loi.

Les établissements situés dans des provinces et territoires qui ne disposent pas de lois sur la protection des renseignements personnels sur la santé sont assujettis aux lois régissant le secteur public. Celles-ci donnent aux établissements le droit de divulguer des renseignements personnels à des fins statistiques sans le consentement de la personne concernée.

Ententes

À l'ICIS, les données du SISD sont régies par la *Politique de respect de la vie privée, 2010*, la législation en vigueur dans les provinces et territoires et les ententes de partage de données conclues avec les provinces et territoires. Les ententes de partage des données établissent les critères relatifs au but, à l'utilisation, à la divulgation, à la conservation et à la destruction des renseignements personnels sur la santé fournis à l'ICIS, ainsi que toute divulgation subséquemment permise. Les ententes décrivent aussi l'autorité législative selon laquelle les renseignements personnels sur la santé sont divulgués à l'ICIS.

3.3 Premier principe : responsabilité à l'égard des renseignements personnels sur la santé

Il incombe au président-directeur général de l'ICIS de s'assurer de la conformité à la *Politique de respect de la vie privée, 2010* de l'ICIS. À cet égard, l'ICIS compte sur une chef de la protection des renseignements personnels et avocate générale, un comité sur le respect de la vie privée, la confidentialité et la sécurité, un comité de gouvernance et de respect de la vie privée issu du Conseil d'administration et un conseiller principal externe à la protection des renseignements personnels.

Organisation et gouvernance

Le tableau ci-dessous présente les principaux postes de direction à l'ICIS responsables de la gestion des risques associés au respect de la vie privée et à la sécurité pour le SISD.

Tableau Principaux postes et responsabilités

Poste ou groupe	Rôles et responsabilités
Vice-président, Stratégies de données et Statistiques	Responsable de l’orientation stratégique générale du SISD
Directeur, Soins spécialisés	Responsable du fonctionnement général du SISD et des décisions administratives stratégiques connexes
Gestionnaire, Gestion des données, Soins spécialisés	Responsable de la gestion quotidienne des données du SISD, y compris la qualité des données et la production de rapports
Chef de la sécurité de l’information	Responsable de l’orientation stratégique et de la mise en œuvre générale du programme de sécurité de l’information de l’ICIS
Chef de la protection des renseignements personnels	Responsable de l’orientation stratégique et de la mise en œuvre générale du programme de respect de la vie privée de l’ICIS

3.4 Deuxième principe : établissement des objectifs de la collecte de renseignements personnels sur la santé

L’ICIS a pour mandat de fournir une information comparable et exploitable qui favorise une amélioration rapide des soins de santé, de la performance des systèmes de santé et de la santé de la population dans l’ensemble du continuum de soins. L’organisme produit notamment de l’information sur les services à domicile afin de soutenir la planification et la gestion de ces services financés par le secteur public au Canada. Pour ce faire, l’ICIS recueille les types suivants de données du SISD aux fins indiquées :

Identificateurs personnels

Il peut s’agir, par exemple, du numéro d’assurance maladie ou d’un identificateur personnel propre au SISD. L’ICIS utilise ces informations pour brosser le portrait complet des soins fournis à la personne en regroupant les enregistrements décrivant les divers types de soins qui lui ont été fournis à divers moments par divers établissements. Afin de pouvoir réunir les enregistrements, l’ICIS doit savoir lesquels se rapportent à la personne. Pour cette raison, tous les enregistrements doivent inclure des identificateurs.

Caractéristiques démographiques

Il peut s’agir, par exemple, de la date de naissance, du code postal, du sexe, de la situation de famille, de la langue, du niveau d’études, du statut d’emploi ou de données identificatoires sur les Autochtones. L’ICIS utilise l’âge (calculé avec la date de naissance), l’information géographique dérivée du code postal, le sexe, la langue, le statut d’emploi et les données identificatoires sur les Autochtones pour réaliser des analyses démographiques des services de santé fournis et de leurs résultats.

Caractéristiques de santé

Il peut s’agir, par exemple, des évaluations des résidents réalisées par les organismes (état de santé, état cognitif et fonctionnel, soins dispensés). L’ICIS se sert de cette information pour évaluer les types de problèmes de santé qui nécessitent des services à domicile, la qualité des services fournis à la personne et les coûts associés aux services.

Données administratives

Il peut s’agir, par exemple, des dates auxquelles les services à domicile ont débuté et pris fin. À l’aide de ces informations, l’ICIS évalue le temps d’attente pour les services, de même que les ressources consommées pour leur prestation.

Identificateurs de l’établissement de santé

Il peut s’agir, par exemple, du nom ou du code du dispensateur qui a fourni les services à domicile. Ces informations permettent à l’ICIS de comparer les dispensateurs de services.

Champs de texte libre

Ces champs permettent de recueillir des données non structurées (p. ex. noms de médicaments). Les champs de texte libre ne doivent pas contenir des renseignements personnels sur la santé. L’ICIS évalue régulièrement le risque qu’un établissement saisisse des renseignements personnels sur la santé (p. ex. numéro d’assurance maladie, nom) dans un champ de texte libre et prend des mesures pour atténuer ce risque (notamment en vérifiant si ces champs contiennent des renseignements personnels sur la santé et en limitant l’accès à ces champs tant à l’interne qu’à l’externe). Les risques associés aux champs de texte libre sont actuellement évalués dans le cadre du programme de gestion des risques liés au respect de la vie privée et à la sécurité de l’ICIS, dont il est question à la section 3.1.

3.5 Troisième principe : consentement pour la collecte, l’utilisation ou la divulgation de renseignements personnels sur la santé

À titre de collecteur secondaire de données, l’ICIS n’a pas de contact direct avec les patients. L’ICIS s’attend à ce que les fournisseurs de données respectent les règles et leurs responsabilités en matière de collecte, d’utilisation et de divulgation de données, y compris en ce qui concerne le consentement et les avis, conformément aux lois, aux règlements et aux politiques en vigueur dans les provinces et territoires.

3.6 Quatrième principe : restriction de la collecte de renseignements personnels sur la santé

L’ICIS souscrit au principe de la minimisation des données. En vertu des articles 1 et 2 de sa *Politique de respect de la vie privée, 2010*, l’ICIS ne recueille des fournisseurs de données que les renseignements raisonnablement nécessaires pour les besoins du système de santé, dont l’analyse statistique et la production de rapports connexes, à des fins de gestion, d’évaluation ou de surveillance des systèmes de santé. Par conséquent, le SISD ne recueille que les données nécessaires à ces fins.

3.7 Cinquième principe : restriction de l’utilisation, de la divulgation et de la conservation des renseignements personnels sur la santé

Restriction de l’utilisation

Clients

L’ICIS restreint l’utilisation des données du SISD aux objectifs autorisés décrits à la section 3.4. Cela comprend les analyses comparatives au sein des provinces et territoires et entre ceux-ci, les analyses des tendances visant à évaluer ou à surveiller l’incidence de tout changement en matière de politiques, de pratiques et de prestation de services, ainsi que la production de statistiques pour appuyer la planification, la gestion et l’amélioration de la qualité.

Personnel de l'ICIS

Le personnel de l'ICIS est autorisé à accéder aux données et à les utiliser uniquement en cas de nécessité, notamment pour la gestion du traitement et de la qualité des données, la production de statistiques et de fichiers de données, ainsi que la réalisation d'analyses. Tous les membres du personnel de l'ICIS doivent signer une entente de confidentialité au moment de leur embauche, et sont ensuite tenus de renouveler chaque année leur engagement à l'égard du respect de la vie privée.

L'accès du personnel à l'environnement analytique SAS est fourni au moyen du processus centralisé d'accès aux données SAS de l'ICIS, qui est géré par le Centre de services de l'ICIS. Cet environnement distinct et sécurisé sert au stockage des fichiers de données analytiques, y compris des fichiers pour usage général, où le personnel doit effectuer ses analyses et en stocker les résultats.

Les fichiers de données pour usage général sont des fichiers prétraités conçus expressément pour les besoins des analystes internes. Le prétraitement consiste à supprimer le numéro d'assurance maladie original (et à le remplacer par un numéro d'assurance maladie non chiffré), la date de naissance complète et le code postal complet, et à les remplacer par un ensemble de variables dérivées standards.

Ce processus garantit que toutes les demandes d'accès, y compris aux données du SISD, sont vérifiables et autorisées, conformément à l'article 10 de la *Politique de respect de la vie privée, 2010* de l'ICIS. Le système d'accès aux données SAS fait l'objet d'une vérification annuelle qui permet de confirmer que les employés accèdent aux données seulement en cas de nécessité. La section 3.9 explique comment les différentes mesures procédurales et techniques sont mises en place en vue de prévenir l'accès non autorisé aux données du SISD et de sécuriser les données de toute autre manière.

Couplage des données

Les données du SISD sont couplées à celles d'autres sources de données de l'ICIS. Comme le couplage des données peut accroître les risques d'identification de la personne, l'ICIS prend des mesures d'atténuation des risques.

Les articles 14 à 31 de la *Politique de respect de la vie privée, 2010* de l'ICIS régissent le couplage des enregistrements contenant des renseignements personnels sur la santé. En vertu de cette politique, l'ICIS permet le couplage des renseignements personnels sur la santé dans certaines circonstances. Il est généralement permis de coupler des données au sein d'une seule banque de données pour l'usage exclusif de l'ICIS. Le couplage de données à partir de multiples banques de données pour l'usage exclusif de l'ICIS et toutes les demandes de couplage de données formulées par des tiers sont soumis à un processus

interne d'examen et d'approbation. Lors du couplage, l'ICIS utilise généralement des numéros d'assurance maladie chiffrés. Les données couplées demeurent assujetties aux dispositions en matière d'utilisation et de divulgation de la *Politique de respect de la vie privée, 2010*.

Les critères d'approbation du couplage de données sont énoncés comme suit aux articles 23 et 24 de la *Politique de respect de la vie privée, 2010* de l'ICIS :

Article 23 Les personnes dont les renseignements personnels sur la santé sont utilisés pour le couplage de données y consentent au préalable; ou

Article 24 Tous les critères suivants sont respectés :

a. l'objectif du couplage de données s'inscrit dans le mandat de l'ICIS;
b. les avantages pour le public sont considérablement plus importants que les risques de violation de la vie privée des personnes;
c. les résultats du couplage de données ne porteront pas préjudice aux personnes concernées;
d. le couplage de données s'inscrit dans un projet précis et ponctuel, et les données couplées seront par la suite détruites dans le respect des règles énoncées aux articles 28 et 29;
e. (peut remplacer le critère d.) le couplage de données est effectué dans le cadre d'un programme de travail continu et approuvé de l'ICIS; les données sont conservées aussi longtemps que nécessaire pour la réalisation des fins déterminées, après quoi elles sont détruites dans le respect des règles énoncées aux articles 28 et 29;
f. le couplage de données permet de réaliser des économies évidentes par rapport à d'autres méthodes ou est l'unique méthode envisageable.

Norme de couplage de données sur les clients

En 2015, l'ICIS a adopté une norme de couplage de données sur les clients à l'échelle de l'organisme. Cette norme régit le couplage des enregistrements qui ont été créés depuis 2010-2011 et qui contiennent les éléments de données suivants : numéro d'assurance maladie chiffré et province ou territoire ayant émis le numéro d'assurance maladie. Les enregistrements qui ne satisfont pas à ces critères sont régis par un mécanisme de couplage défini au cas par cas.

Destruction des données couplées

L'article 28 de la *Politique de respect de la vie privée, 2010* de l'ICIS définit l'exigence selon laquelle l'ICIS doit détruire les renseignements personnels sur la santé et les données dépersonnalisées de façon sécuritaire, à l'aide de méthodes de destruction qui conviennent au format, au support ou au dispositif, de manière à ce qu'une reconstitution ne soit pas raisonnablement prévisible.

Pour certains projets ponctuels, l'article 29 de la *Politique de respect de la vie privée, 2010* de l'ICIS prévoit par ailleurs que la destruction sécuritaire des données couplées aura lieu dans l'année suivant la publication de l'analyse ou dans les 3 années suivant le couplage, selon la première éventualité, conformément à la *norme de destruction sécuritaire* de l'ICIS. S'il s'agit de données couplées dans le cadre d'un programme de travail continu, une destruction sécuritaire doit avoir lieu lorsque les données ne sont plus nécessaires pour la réalisation des fins déterminées, conformément à la *norme de destruction sécuritaire* de l'ICIS. Cette exigence s'applique au couplage de données tant pour l'usage exclusif de l'ICIS que pour les demandes formulées par des tiers.

Renvoi des données au fournisseur

Un organisme déclarant peut accéder aux rapports de soumission en ligne sécurisés, qui indiquent combien d'enregistrements l'organisme a soumis avec succès au SISD. Ces rapports précisent également quels enregistrements ont été rejetés et pour quelle raison (p. ex. information manquante). Ils permettent à l'organisme de cerner et de corriger les erreurs, puis de soumettre de nouveau les enregistrements. Le rapport utilise l'identificateur que l'organisme a attribué à chaque client (le rapport ne contient aucun numéro d'assurance maladie) pour identifier les enregistrements problématiques.

L'article 34 de la *Politique de respect de la vie privée, 2010* stipule que l'ICIS, en plus de renvoyer les données aux établissements déclarants, peut également remettre les enregistrements au ministère concerné, pour des motifs de qualité des données ou à d'autres fins inscrites dans son mandat (p. ex. la gestion des services de santé et de la santé de la population, qui comprend la planification, l'évaluation et l'affectation des ressources) ou tel qu'il est indiqué dans l'entente de partage des données ou un autre instrument juridique. Le renvoi des données au fournisseur de données est considéré comme une utilisation et non comme une divulgation.

Restriction de la divulgation

Chaque trimestre, l'ICIS fournit des rapports électroniques comparatifs du SISD à tous les fournisseurs de données. Ces rapports contiennent des données agrégées permettant d'identifier un établissement grâce auxquelles les fournisseurs de données peuvent analyser leurs données au fil du temps et se comparer à d'autres dispensateurs de services semblables au pays.

Avant d'avoir accès aux rapports électroniques du SISD, les organismes doivent signer l'*Entente de services de rapports électroniques* de l'ICIS qui comprend notamment des règles visant à

- restreindre l'utilisation de l'information à des fins non commerciales aux activités de gestion interne, d'assurance de la qualité des données, de planification, de recherche, d'analyse ou d'appui à la prise de décisions reposant sur des données probantes des organismes;
- interdire la divulgation des données à des tiers, sauf s'il s'agit des données de l'organisme;
- permettre la publication de l'information uniquement lorsque toutes les mesures raisonnables ont été prises pour préserver l'identité des personnes et que les données ne contiennent pas de cellules comprenant moins de 5 observations;
- interdire la publication de renseignements permettant d'identifier un établissement ou organisme de santé, à moins que l'organisme en informe préalablement l'ICIS afin de lui permettre d'aviser le ministère concerné.

Demandes de données formulées par des tiers

Des tiers peuvent demander qu'on leur fournisse des données au niveau de l'enregistrement ou des données agrégées sur mesure provenant du SISD.

L'ICIS administre le programme de demandes de données par des tiers, qui établit les mesures de contrôle appropriées de respect de la vie privée et de la sécurité que l'organisme demandeur doit respecter. En outre, comme le stipulent les articles 37 à 57 de sa *Politique de respect de la vie privée, 2010*, l'ICIS divulgue des renseignements sur la santé conformément à son mandat et à ses fonctions de base, et s'efforce de divulguer les données dans le plus grand anonymat possible tout en répondant aux exigences de recherche ou d'analyse du demandeur. Cela signifie que les données sont agrégées dans la mesure du possible. Si les données agrégées ne sont pas suffisamment détaillées pour les besoins définis, l'ICIS peut décider, au cas par cas, de divulguer au destinataire des données dépersonnalisées au niveau de l'enregistrement ou des renseignements personnels sur la santé (dans des circonstances particulières, par exemple, avec le consentement de la personne). Le destinataire doit avoir signé au préalable une entente de protection des données ou un autre instrument juridiquement contraignant avec l'ICIS. Seuls les éléments de données nécessaires aux fins prévues seront divulgués.

L'ICIS utilise un environnement d'accès sécurisé (EAS) comme moyen d'accès privilégié aux données au niveau de l'enregistrement. L'EAS est un environnement chiffré et sécurisé hébergé dans le centre des données de l'ICIS. Conformément aux politiques et procédures en vigueur à l'ICIS, les chercheurs autorisés — qui sont liés par de rigoureuses conditions d'utilisation — ont accès à des données extraites, préparées et vérifiées par des membres du personnel de l'ICIS pour un projet de recherche approuvé. Les données au niveau de

l'enregistrement ne peuvent pas être copiées ni extraites de l'EAS; seuls des résultats agrégés peuvent être extraits de l'EAS. De plus amples renseignements sur l'EAS sont disponibles sur le site Web de l'ICIS (à la page Faire une demande de données et dans le document Évaluation des incidences sur la vie privée de l'*environnement d'accès sécurisé*).

Dans les cas où l'ICIS a accordé aux chercheurs et autres utilisateurs autorisés l'accès à des données au niveau de l'enregistrement en extrayant les données pertinentes dans des fichiers transmis aux utilisateurs, l'ICIS a adopté une approche de gestion axée sur le cycle de vie en ce qui a trait aux demandes de données au niveau de l'enregistrement provenant de tiers. Le Secrétariat à la vie privée et aux services juridiques a élaboré et gère un processus de surveillance continue de la conformité qui fait partie intégrante de ce cycle de vie. Dans le cadre de ce processus, tous les fichiers de données qui sont divulgués à des demandeurs tiers font l'objet d'un suivi et d'une surveillance de façon à garantir leur destruction sécuritaire à la fin de leur cycle de vie. Avant d'avoir accès aux données, les demandeurs tiers doivent signer une entente de protection des données et accepter de se conformer aux conditions et restrictions de l'ICIS concernant la collecte, le but, l'utilisation, la sécurité, la divulgation et le renvoi ou la destruction des données.

Les demandeurs de données sont tenus de remplir et soumettre un formulaire de demande. Ils sont également tenus de signer une entente en vertu de laquelle ils s'engagent à utiliser les données uniquement aux fins précisées. Toutes les ententes de protection des données conclues avec des tiers stipulent que les organismes destinataires doivent veiller à la stricte confidentialité des données au niveau de l'enregistrement et qu'ils ne doivent pas divulguer ces données à des personnes en dehors de l'organisme. L'ICIS impose en outre des obligations à ces tiers destinataires, notamment

- des exigences de destruction sécuritaire;
- le droit de l'ICIS de procéder à des vérifications;
- l'interdiction de publier des cellules comprenant moins de 5 observations;
- une solide technologie de cryptage satisfaisant aux normes de l'ICIS ou les surpassant si des appareils informatiques mobiles sont utilisés.

Outre le processus de surveillance continue de la conformité — qui consiste à s'assurer que les fichiers de données divulgués à des tiers destinataires font l'objet d'un suivi et d'une surveillance jusqu'à leur destruction sécuritaire à la fin de leur cycle de vie —, le Secrétariat à la vie privée et aux services juridiques communique chaque année avec les tiers destinataires de données pour vérifier qu'ils respectent toujours les obligations énoncées dans le formulaire de demande de données et l'entente de protection des données de l'ICIS qu'ils ont signée.

Comme indiqué à la section 3.4 de la présente évaluation des incidences sur la vie privée, le SISD contient un champ destiné aux données identificatoires sur les Autochtones. La divulgation de cet identificateur est soumise à la *politique sur la diffusion et la divulgation de données identificatoires sur les Autochtones* de l'ICIS, en vertu de laquelle toute demande de données identifiant des Autochtones doit être accompagnée d'une preuve de l'approbation des autorités autochtones compétentes. Pour en savoir plus, consultez le document *Tracer la voie vers la gouvernance respectueuse des données de l'ICIS sur les Premières Nations, les Inuits et les Métis*, et la page Premières Nations, Inuits et Métis sur le site Web de l'ICIS.

Contrat de licence avec interRAI

L'ICIS a signé un contrat de licence avec interRAI, un réseau regroupant des chercheurs et des praticiens dont l'objectif est d'améliorer les soins de santé pour les personnes handicapées ou présentant des besoins médicaux complexes. Cette licence accorde à l'ICIS le droit exclusif d'utiliser les formulaires d'évaluation d'interRAI au Canada aux fins de production de rapports statistiques à l'échelle nationale. Le contrat de licence engage également l'ICIS à fournir à interRAI, sur une base annuelle, une copie dépersonnalisée des données recueillies au moyen des formulaires d'évaluation interRAI et soumises au SISD. Par conséquent, l'ICIS fournit à interRAI des données dépersonnalisées provenant du SISD en vertu d'une entente de partage des données, qui indique les raisons pour lesquelles interRAI peut utiliser les données (p. ex. pour élaborer des formulaires d'évaluation), ainsi que les responsabilités d'interRAI en matière de protection des données.

Diffusion publique

Dans le cadre de son mandat, l'ICIS publie uniquement des données agrégées en s'assurant de réduire au minimum le risque d'identification et de divulgation par recoupements. En général, il faut au moins 5 observations par cellule conformément à l'article 33 de la *Politique de respect de la vie privée, 2010* de l'ICIS. Des statistiques agrégées et des analyses sont publiées dans les documents et sur le site Web de l'ICIS au moyen d'outils comme Votre système de santé : En détail et les Statistiques éclair, ainsi que les indicateurs sur les priorités partagées en santé.

Restriction de la conservation

Le SISD fait partie des banques de données de l'ICIS. Conformément à son mandat et à ses fonctions de base, l'ICIS conserve les données de ce système aussi longtemps que nécessaire pour la réalisation des fins déterminées.

3.8 Sixième principe : exactitude des renseignements personnels sur la santé

L'ICIS dispose d'un programme complet sur la qualité des données. Tout problème connu de qualité des données doit être réglé par le fournisseur de données ou consigné dans la documentation sur les limites des données, que l'ICIS fournit à tous les utilisateurs.

À l'instar d'autres banques de données de l'ICIS, le SISD doit régulièrement faire l'objet d'une évaluation de la qualité des données fondée sur le *Cadre de la qualité de l'information de l'ICIS*. Ce processus comprend de nombreuses activités visant à évaluer les diverses dimensions de la qualité, dont l'exactitude des données du SISD.

3.9 Septième principe : mesures de protection des renseignements personnels sur la santé

Cadre de respect de la vie privée et de sécurité de l'ICIS

L'ICIS a élaboré un *Cadre de respect de la vie privée et de sécurité* visant à offrir une approche globale de la gestion du respect de la vie privée et de la sécurité. Ce cadre est fondé sur des pratiques exemplaires des secteurs public et privé ainsi que du secteur de la santé. Il est conçu de façon à coordonner les politiques de l'ICIS en matière de respect de la vie privée et de sécurité, et à offrir une vision intégrée des pratiques de gestion de l'information adoptées par l'organisme. Les paragraphes qui suivent décrivent les aspects de la sécurité des systèmes de l'ICIS qui revêtent une importance particulière au regard du SISD.

Sécurité des systèmes

L'ICIS reconnaît que l'information ne peut être considérée comme sécurisée que si elle est protégée pendant tout son cycle de vie, c'est-à-dire à chaque étape des processus de création, de collecte, d'accès, de conservation, de stockage, d'utilisation, de divulgation et de destruction. Par conséquent, l'ICIS dispose de toute une série de politiques qui définissent les contrôles nécessaires pour garantir la protection de l'information en format physique et électronique, y compris des mesures rigoureuses de chiffrement et d'élimination. Ces politiques ainsi que les normes, lignes directrices et procédures opérationnelles qui s'y rattachent sont conformes aux pratiques exemplaires en matière de respect de la vie privée, de sécurité de l'information et de gestion des enregistrements, afin de garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels de l'ICIS.

Les registres de contrôle et de vérification du système font partie intégrante du programme de sécurité de l’information de l’ICIS. Ces registres sont par ailleurs immuables. En général, l’ICIS utilise des données dépersonnalisées au niveau de l’enregistrement (où le numéro d’assurance maladie a été supprimé ou chiffré) pour réaliser ses analyses. Il arrive dans des circonstances exceptionnelles que le personnel doive avoir accès aux numéros d’assurance maladie d’origine. Les procédures et la *Politique de respect de la vie privée, 2010* de l’ICIS prévoient des contrôles stricts qui garantissent que l’accès est autorisé dans les circonstances et au niveau appropriés, et que le principe de minimisation des données est respecté en tout temps. L’ICIS consigne dans ses registres les activités suivantes ayant trait à l’accès aux données :

- l’accès aux numéros d’assurance maladie et aux noms des patients (rarement recueillis) dans les bases de données de production de l’ICIS;
- l’accès aux fichiers de données contenant des renseignements personnels sur la santé qui sont extraits des bases de données de production de l’ICIS et mis à la disposition des analystes internes dans des circonstances exceptionnelles;
- la modification des privilèges d’accès dans les bases de données de production.

Les employés de l’ICIS sont sensibilisés à l’importance de maintenir la confidentialité des renseignements personnels sur la santé et d’autres types d’information sensible au moyen d’un programme de formation obligatoire sur le respect de la vie privée et la sécurité, et par l’intermédiaire de communications continues concernant les politiques et procédures de l’ICIS à ce sujet. Avant chaque tentative de connexion à un système d’information de l’ICIS, les employés doivent confirmer qu’ils comprennent l’interdiction d’accéder à ce système informatique ou de l’utiliser sans autorisation expresse de l’ICIS ni au-delà de cette autorisation.

L’ICIS s’emploie à protéger son système de technologies de l’information, à sécuriser ses banques de données ainsi qu’à protéger les renseignements sur la santé en sa possession au moyen de mesures de sécurité administratives, physiques et techniques appropriées, selon la sensibilité de l’information. Les vérifications représentent une composante importante du programme global de sécurité de l’information de l’ICIS; elles visent à assurer le respect des pratiques exemplaires et à mesurer la conformité avec l’ensemble des politiques, des procédures et des pratiques de sécurité de l’information mises en œuvre par l’ICIS. Les vérifications servent entre autres à évaluer la conformité, sur le plan technique, des systèmes de traitement de l’information aux pratiques exemplaires ainsi qu’aux normes de sécurité et aux normes architecturales connues; la capacité de l’ICIS à protéger l’information et les systèmes de traitement de l’information contre les menaces et vulnérabilités; et la posture de sécurité globale de l’infrastructure technique de l’ICIS, notamment les réseaux, les serveurs, les coupe-feu, les logiciels et les applications.

Les évaluations de la vulnérabilité et les tests d'intrusion de son infrastructure et de certaines applications, effectués par des tiers sur une base régulière, constituent une composante importante du programme de vérification de l'ICIS. Toutes les recommandations issues de vérifications par des tiers sont consignées dans le registre des recommandations du plan d'action général de l'ICIS, et les mesures sont prises en conséquence.

3.10 Huitième principe : transparence de la gestion des renseignements personnels sur la santé

L'ICIS publie de l'information concernant ses politiques sur le respect de la vie privée, ses pratiques relatives aux données et ses programmes de gestion des renseignements personnels sur la santé. Plus précisément, le *Cadre de respect de la vie privée et de sécurité* et la *Politique de respect de la vie privée, 2010* de l'ICIS sont accessibles sur son site Web (icis.ca).

3.11 Neuvième principe : accès individuel aux renseignements personnels sur la santé et modification de ceux-ci

L'ICIS n'utilise pas les renseignements personnels sur la santé en sa possession pour prendre des décisions administratives ou relatives aux personnes concernées. Toute personne qui souhaite accéder à ses renseignements personnels sur la santé verra sa demande traitée conformément aux articles 60 à 63 de la *Politique de respect de la vie privée, 2010* de l'ICIS.

3.12 Dixième principe : plaintes concernant le traitement par l'ICIS des renseignements personnels sur la santé

Comme le précisent les articles 64 et 65 de la *Politique de respect de la vie privée, 2010* de l'ICIS, les plaintes, questions et préoccupations concernant le traitement des renseignements par l'ICIS sont examinées par la chef de la protection des renseignements personnels, qui peut acheminer une demande ou une plainte au commissaire à la protection de la vie privée de la province ou du territoire de l'auteur de la demande ou de la plainte.

4 Conclusion

L’évaluation du SISD effectuée par l’ICIS n’a relevé aucun risque lié au respect de la vie privée et à la sécurité.

La présente évaluation sera mise à jour ou révisée conformément à la *Politique d’évaluation des incidences sur la vie privée* de l’ICIS.

Annexe

Texte de remplacement pour la figure

Figure 1 : Cheminement des données du SISD

Le cheminement des données du SISD va comme suit :

1. L’organisme soumet les enregistrements à l’ICIS. Dans certains cas, les enregistrements sont soumis par un ministère ou une autorité sanitaire.
2. Le SISD transmet des rapports de soumission pour aider l’organisme à corriger les erreurs relevées dans les enregistrements (p. ex. éléments de données manquants).
3. Une copie des enregistrements tels qu’ils ont été acceptés par le SISD ainsi que certains rapports qui comprennent des renseignements personnels sur la santé sont mis à la disposition de l’organisme, du ministère et de l’autorité sanitaire régionale, selon le cas.
4. L’ICIS fournit, au moyen des rapports électroniques du SISD, des données agrégées aux organismes qui soumettent des données au SISD, aux autorités sanitaires et au ministère.
5. Le SISD peut divulguer des données agrégées et dépersonnalisées au niveau de l’enregistrement aux tiers qui en font la demande.
6. Le SISD divulgue des données agrégées au public.

aide@icis.ca

ICIS Ottawa
495, chemin Richmond
Bureau 600
Ottawa (Ont.)
K2A 4H6
613-241-7860

ICIS Toronto
4110, rue Yonge
Bureau 300
Toronto (Ont.)
M2P 2B7
416-481-2002

ICIS Victoria
880, rue Douglas
Bureau 600
Victoria (C.-B.)
V8W 2B7
250-220-4100

ICIS Montréal
1010, rue Sherbrooke Ouest
Bureau 602
Montréal (Qc)
H3A 2R7
514-842-2226

icis.ca

18615-0622